BEZPEČNOSTNÝ BULLETIN

Týždeň 29. 11. 2023 - 05. 12. 2023

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	WPS Software WPS Office - bezpečnostná zraniteľnosť	Vysoká	**8.8**
02.	Apache Superset - bezpečnostná zraniteľnosť	Vysoká	**8.8**
03.	Chrome - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
04.	Apache ActiveMQ - bezpečnostná zraniteľnosť	Vysoká	**8.8**
05.	Apple produkty - viacero bezpečnostných zraniteľností	Vysoká	**8.8**
06.	GitLab - viacero bezpečnostných zraniteľností	Vysoká	**8.7**
07.	Trellix Application and Change Control - bezpečnostná zraniteľnosť	Vysoká	**8.4**
08.	IBM produkty - tri bezpečnostné zraniteľnosti	Vysoká	**8.4**
09.	Foxit PDF Reader a PDF Editor - viacero bezpečnostných zraniteľností	Vysoká	**7.8**
10.	Delta Electronics DOPSoft - bezpečnostná zraniteľnosť	Vysoká	**7.8**
11.	Mitsubishi Electric FA Engineering Software - bezpečnostná zraniteľnosť	Vysoká	**7.8**
12.	Asana Desktop - kritická bezpečnostná zraniteľnosť	Vysoká	**7.7**
13.	Zyxel firewally a AP - bezpečnostné zraniteľnosti	Vysoká	**7.5**
14.	LOYTEC electronics LINX Configurator - tri bezpečnostné zraniteľnosti	Vysoká	**7.5**
15.	BVRP Software SLmail - tri bezpečnostné zraniteľnosti	Vysoká	**7.5**
16.	Neutron IP Camera - bezpečnostná zraniteľnosť	Vysoká	**7.5**
17.	OpenZFS - bezpečnostná zraniteľnosť	Vysoká	**7.5**
18.	Dell RVTools - bezpečnostná zraniteľnosť	Vysoká	**7.5**
19.	Tecno Mobile 4G Portable WiFi TR118 - bezpečnostná zraniteľnosť	Vysoká	**7.2**
20.	Progress MOVEit Transfer - dve bezpečnostné zraniteľnosti	Vysoká	**7.2**
21.	Chipsety ASR1803 a ASR1806 - kritická bezpečnostná zraniteľnosť	Vysoká	**7.2**
22.	Warptech Industries Warpgate - bezpečnostná zraniteľnosť	Vysoká	**7.1**
23.	Jenkins pluginy - viacero bezpečnostných zraniteľností	Vysoká	**7.1**
24.	Bluetooth Core Specification - bezpečnostná zraniteľnosť	Stredná	**6.8**
25.	Franklin Electric Fueling Systems Colibri - bezpečnostná zraniteľnosť	Stredná	**6.5**
26.	BD FACSChorus - viacero bezpečnostných zraniteľností	Stredná	**5.4**
27.	Yokogawa STARDOM - bezpečnostná zraniteľnosť	Stredná	**5.3**
28.	Mitsubishi Electric GX Works2 - dve bezpečnostné zraniteľnosti	Nízka	**2.5**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01794/2022/SK-CERT-1437

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WPS Software WPS Office - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu WPS Office.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-31275

Zasiahnuté systémy

WPS Office vo verzii staršej ako 11.2.0.11537 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.talosintelligence.com/vulnerability_reports/TALOS-2023-1748

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Superset - bezpečnostná zraniteľnosť

Popis

Vývojári platformy Apache Superset vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii mechanizmov autentifikácie a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-40610

Zasiahnuté systémy

Apache Superset vo verzii staršej ako 2.1.2

Následky

Eskalácia privilégií
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://lists.apache.org/thread/jvgxpk4dbxyqtsgtl4pdgbd520rc0rot
https://exchange.xforce.ibmcloud.com/vulnerabilities/272252

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Chrome - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Google vydala bezpečnostnú aktualizáciu na svoj webový prehliadač Google Chrome, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.11.2023

CVE

CVE-2023-6345, CVE-2023-6346, CVE-2023-6347, CVE-2023-6348, CVE-2023-6350, CVE-2023-6351

Zasiahnuté systémy

Chrome pre Mac a Linux vo verzii staršej ako 119.0.6045.199
Chrome pre Windows vo verzii staršej ako 119.0.6045.199/.200

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://chromereleases.googleblog.com/2023/11/stable-channel-update-for-desktop_28.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache ActiveMQ - bezpečnostná zraniteľnosť

Popis

Vývojári protokolu Apache ActiveMQ vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov v rámci komponentu Jolokia a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2022-41678

Zasiahnuté systémy

Apache ActiveMQ vo verzii staršej ako 5.16.6, 5.17.4

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://seclists.org/oss-sec/2023/q4/241
https://exchange.xforce.ibmcloud.com/vulnerabilities/272445

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apple produkty - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Apple vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente WebKit, zasahuje Safari, macOS Sonoma, iOS a iPadOS a spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorenej webovej stránky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-42916, CVE-2023-42917

Zasiahnuté systémy

macOS Sonoma vo verzii staršej ako 14.1.2
iOS vo verzii staršej ako 17.1.2
iPadOS vo verzii staršej ako 17.1.2
Safari vo verzii staršej ako 17.1.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://support.apple.com/en-us/HT214032
https://support.apple.com/en-us/HT214031
https://support.apple.com/en-us/HT214033
https://exchange.xforce.ibmcloud.com/vulnerabilities/272642

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

GitLab - viacero bezpečnostných zraniteľností

Popis

Vývojári platformy GitLab vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v komponente Jira integration, spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa vykonať XSS útok a následne získať neoprávnený prístup k citlivým údajom alebo spôsobiť neoprávnené zmeny v systéme.
Ostatné zraniteľnosti možno zneužiť na získanie neoprávneného prístupu k citlivým údajom, vykonanie neoprávnených zmien v systéme alebo na zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2022-41409, CVE-2023-3401, CVE-2023-3443, CVE-2023-39417, CVE-2023-3949, CVE-2023-3964, CVE-2023-4317, CVE-2023-4658, CVE-2023-4912, CVE-2023-5226, CVE-2023-5995, CVE-2023-6033, CVE-2023-6396

Zasiahnuté systémy

GitLab Community Edition a Enterprise Edition vo verzii staršej ako 16.6.1, 16.5.3, a 16.4.3

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme
Vykonanie škodlivého kódu
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://about.gitlab.com/releases/2023/11/30/security-release-gitlab-16-6-1-released/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Trellix Application and Change Control - bezpečnostná zraniteľnosť

Popis

Spoločnosť Trellix vydala bezpečnostnú aktualizáciu na svoj produkt Application and Change Control, ktorá opravuje bezpečnostnú zraniteľnosť.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v rámci rozšírenia ePO a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-5607

Zasiahnuté systémy

Trellix Application and Change Control (TACC) vo verzii staršej ako 8.4.0

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://kcm.trellix.com/corporate/index?page=content&id=SB10411

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

IBM produkty - tri bezpečnostné zraniteľnosti

Popis

Spoločnosť IBM vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú 4 bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v produkte AIX, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-38003, CVE-2023-42004, CVE-2023-42006, CVE-2023-45168

Zasiahnuté systémy

IBM Security Guardium 11.3
IBM Administration Runtime Expert
IBM Db2 pre Linux, UNIX a Windows (vrátane Db2 Connect Server)
IBM AIX

Kompletnú špecifikáciu zasiahnutých produktov môžete nájsť na stránkach výrobcu v časti ZDROJE.

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.ibm.com/support/pages/node/7069241
https://www.ibm.com/support/pages/node/7085891
https://www.ibm.com/support/pages/node/7078681
https://www.ibm.com/support/pages/node/7086090

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Foxit PDF Reader a PDF Editor - viacero bezpečnostných zraniteľností

Popis

Spoločnosť Foxit vydala bezpečnostné aktualizácie na produkty PDF Reader a PDF Editor, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť sa nachádza v programe PDF Reader, spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-32616, CVE-2023-35985, CVE-2023-38573, CVE-2023-40194, CVE-2023-41257

Zasiahnuté systémy

Foxit PDF Reader vo verzii staršej ako 2023.3
Foxit PDF Editor vo verzii staršej ako 2023.3

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.foxit.com/support/security-bulletins.html
https://exchange.xforce.ibmcloud.com/vulnerabilities/272326

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Delta Electronics DOPSoft - bezpečnostná zraniteľnosť

Popis

Spoločnosť Delta Electronics zverejnila informácie o bezpečnostnej zraniteľnosti svojho produktu DOPSoft.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej kontrole používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-5944

Zasiahnuté systémy

Delta Electronics DOPSoft vo všetkých verziách (ukončená podpora)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame postupovať podľa pokynov výrobcu a prejsť na iný produkt s platnou podporou.

Po odstránení zraniteľností, ktoré mohli spôsobiť vykonanie škodlivého kódu je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-334-01
https://diastudio.deltaww.com/home/downloads?sec=download#catalog

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric FA Engineering Software - bezpečnostná zraniteľnosť

Popis

Spoločnosť Mitsubishi Electric zverejnila informácie o bezpečnostnej zraniteľnosti svojich produktov GX Works3, MELSOFT iQ AppPortal, MELSOFT Navigator a Motion Control Setting.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej kontrole používateľských vstupov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvorených súborov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-5247

Zasiahnuté systémy

GX Works3 vo všetkých verziách
MELSOFT iQ AppPortal vo všetkých verziách
MELSOFT Navigator vo všetkých verziách
Motion Control Setting vo všetkých verziách

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame zraniteľnosti mitigovať podľa odporúčaní od výrobcu, sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať. Detailné inštrukcie môžete nájsť na webovej adrese:
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-016_en.pdf
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-334-04
https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-016_en.pdf

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.7
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Asana Desktop - kritická bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu Asana Desktop.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

28.11.2023

CVE

CVE-2023-49314

Zasiahnuté systémy

Asana Desktop pre macOS vo verzii staršej ako 2.1.0 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Na uvedenú zraniteľnosť v súčasnosti nie sú dostupné bezpečnostné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/louiselalanne/CVE-2023-49314
https://exchange.xforce.ibmcloud.com/vulnerabilities/272572
https://www.tenable.com/cve/CVE-2023-49314

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zyxel firewally a AP - bezpečnostné zraniteľnosti

Popis

Spoločnosť Zyxel vydala bezpečnostné aktualizácie na svoje portfólio firewallov a AP, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť nachádzajúca sa vo firmware zariadení Zyxel ATP spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v rámci QuickSec IPSec toolkit-u a vzdialený neautentifikovaný útočník by ju prostredníctvom zaslania špeciálne vytvoreného IKE paketu mohol zneužiť na zneprístupnenie služby.
Ostatné zraniteľnosti by útočník mohol zneužiť na získanie neoprávneného prístupu k citlivým údajom a realizáciu XSS útokov

Dátum prvého zverejnenia varovania

28.11.2023

CVE

CVE-2023-35136, CVE-2023-35139, CVE-2023-37925, CVE-2023-37926, CVE-2023-4397, CVE-2023-4398, CVE-2023-5650, CVE-2023-5797, CVE-2023-5960

Zasiahnuté systémy

Zyxel firewally série ATP, USG FLEX, USG FLEX 50(W) / USG20(W)-VPN, VPN

Zyxel AP modely NWA50AX, NWA50AX-PRO, NWA55AXE, NWA90AX, NWA90AX-PRO, NWA110AX, NWA210AX, NWA220AX-6E, NWA1123ACv3, WAC500, WAC500H, WAX300H, WAX510D, WAX610D, WAX620D-6E, WAX630S, WAX640S-6E, WAX650S, WAX655E, WBE660S

Presnú špecifikáciu jednotlivých zasiahnutých produktov nájdete na odkaze v časti ZDROJE.

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu
Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-vulnerabilities-in-firewalls-and-aps

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

LOYTEC electronics LINX Configurator - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu LOYTEC electronics LINX Configurator.
Najzávažnejšie zraniteľnosti spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom odpočúvania sieťovej prevádzky získať neoprávnený prístup k prihlasovacím údajom, ktoré by následne mohol zneužiť na získanie neoprávneného prístupu do systému.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-46383, CVE-2023-46384, CVE-2023-46385

Zasiahnuté systémy

LOYTEC electronics GmbH LINX Configurator vo verzii staršej ako 7.4.10 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://seclists.org/fulldisclosure/2023/Nov/6
https://exchange.xforce.ibmcloud.com/vulnerabilities/272313

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BVRP Software SLmail - tri bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu BVRP Software SLmail.
Najzávažnejšia bezpečnostná zraniteľnosť s označením CVE-2023-4595 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.
Ostatné zraniteľnosti je možné zneužiť na získanie neoprávneného prístupu k citlivým údajom a na vykonanie XSS (Cross Site Scripting) útokov.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-4593, CVE-2023-4594, CVE-2023-4595

Zasiahnuté systémy

Slmail vo verzii staršej ako 5.5.0.4433 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Vykonanie škodlivého kódu

Odporúčania

Na uvedené zraniteľnosti v súčasnosti nie sú dostupné aktualizácie. Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.incibe.es/en/incibe-cert/notices/aviso/multiple-vulnerabilities-bvrp-software-slmail
https://exchange.xforce.ibmcloud.com/vulnerabilities/272267

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Neutron IP Camera - bezpečnostná zraniteľnosť

Popis

Spoločnosť Neutron vydala bezpečnostnú aktualizáciu na svoj produkt IP Camera, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-6118

Zasiahnuté systémy

Neutron IP Camera vo verzii firmvéru staršej ako b1130.1.0.1

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/272331

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

OpenZFS - bezpečnostná zraniteľnosť

Popis

Vývojári projektu OpenZFS vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvorenej požiadavky deaktivovať bezpečnostné mechanizmy a vykonať neoprávnené zmeny v systéme.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-49298

Zasiahnuté systémy

OpenZFS vo verzii staršej ako FreeBSD-EN-23:16.openzfs

Následky

Neoprávnená zmena v systéme

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://github.com/openzfs/zfs/pull/15571
https://www.freebsd.org/security/advisories/FreeBSD-EN-23:16.openzfs.asc
https://exchange.xforce.ibmcloud.com/vulnerabilities/272344

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dell RVTools - bezpečnostná zraniteľnosť

Popis

Spoločnosť Dell vydala bezpečnostnú aktualizáciu na svoj produkt RVTools, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť s označením CVE-2023-44303 spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi získať neoprávnený prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-44303

Zasiahnuté systémy

Dell RVTools vo verziách novších ako 3.9.2 a starších ako 4.5.0

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.dell.com/support/kbdoc/en-us/000219712/dsa-2023-426-security-update-for-rvtools-vulnerabilities

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Tecno Mobile 4G Portable WiFi TR118 - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti produktu 4G Portable WiFi TR118.
Bezpečnostná zraniteľnosť nachádzajúca sa v komponente Ping Tool spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora prostredníctvom injekcie špeciálne upravených príkazov vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.
Na uvedenú zraniteľnosť je v súčasnosti voľne dostupný Proof-of-Concept kód.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-6304

Zasiahnuté systémy

Tecno Mobile 4G Portable WiFi TR118 vo verzii firmvéru staršej ako TR118-M30E-RR-D-EnFrArSwHaPo-OP-V008-20220830

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Vzhľadom na to, že produkt už nie je udržiavaný, odporúčame prejsť na iný produkt s platnou podporou.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/272293
https://www.cve.org/CVERecord?id=CVE-2023-6304

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Progress MOVEit Transfer - dve bezpečnostné zraniteľnosti

Popis

Spoločnosť Progress vydala bezpečnostnú aktualizáciu na svoj produkt MOVEit Transfer, ktorá opravuje dve bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami administrátora eskalovať privilégiá iného používateľa na úroveň administrátorského prístupu a spôsobiť úplné narušenie dôvernosti, integrity a dostupnosti systému.
Druhú zraniteľnosť možno zneužiť na realizáciu XSS (Cross Site Scripting) útokov.

Dátum prvého zverejnenia varovania

29.11.2023

CVE

CVE-2023-6217, CVE-2023-6218

Zasiahnuté systémy

MOVEit Transfer vo verzii staršej ako 2023.1.2
MOVEit Transfer vo verzii staršej ako 2023.0.7
MOVEit Transfer vo verzii staršej ako 2022.1.10
MOVEit Transfer vo verzii staršej ako 2022.0.9
MOVEit Transfer vo verzii staršej ako 2021.1.x (13.1.x) (vrátane)

Následky

Eskalácia privilégií
Vykonanie škodlivého kódu

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://community.progress.com/s/article/MOVEit-Transfer-Service-Pack-November-2023

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.2
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Chipsety ASR1803 a ASR1806 - kritická bezpečnostná zraniteľnosť

Popis

Spoločnosť ASR Microelectronics vydala bezpečnostnú aktualizáciu firmvéru na svoje chipsety pre modemy ASR1803 a ASR1806, ktorá opravuje tri bezpečnostné zraniteľnosti, z ktorých jedna označená ako kritická.

Kritická bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov v rámci komponentu SIM Management a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zneužitia out-of-bounds zápisu vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-49699, CVE-2023-49700, CVE-2023-49701

Zasiahnuté systémy

ASR1803 vo verzii firmvéru staršej ako CP01.057.063
ASR1806 vo verzii firmvéru staršej ako CP01.057.063

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame bezodkladne vykonať aktualizáciu firmvéru zasiahnutých systémov.

Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.asrmicro.com/en/goods/psirt?cid=31
https://nvd.nist.gov/vuln/detail/CVE-2023-49701

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Warptech Industries Warpgate - bezpečnostná zraniteľnosť

Popis

Spoločnosť Warptech Industries vydala bezpečnostnú aktualizáciu na svoj produkt Warpgate, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa, ktorý sa nachádza v rovnakom sieťovom segmente prostredníctvom zaslania špeciálne vytvorenej požiadavky eskalovať svoje privilégiá a následne získať neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

23.11.2023

CVE

CVE-2023-48712

Zasiahnuté systémy

Warpgate vo verzii staršej ako 0.9.0

Následky

Eskalácia privilégií
Neoprávnený prístup do systému
Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://github.com/warp-tech/warpgate/security/advisories/GHSA-c94j-vqr5-3mxr
https://exchange.xforce.ibmcloud.com/vulnerabilities/272350

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.1
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Jenkins pluginy - viacero bezpečnostných zraniteľností

Popis

Vývojári JENKINS pluginov MATLAB, Jira, Google Compute Engine a NeuVector Vulnerability Scanner vydali bezpečnostné aktualizácie svojich produktov, ktoré opravujú tri viacero bezpečnostných zraniteľností.
Najzávažnejšie zraniteľnosti sa nachádzajú v plugine MATLAB, spočívajú v nedostatočnej implementácii bezpečnostných mechanizmov a umožňujú vzdialenému, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne vytvorenej požiadavky získať neoprávnený prístup k citlivým údajom a realizáciu CSRF (Cross Site Request Forgery) a XXE (XML External Entity) útokov.

Dátum prvého zverejnenia varovania

29.11.2023

CVE

CVE-2023-49652, CVE-2023-49653, CVE-2023-49654, CVE-2023-49655, CVE-2023-49656, CVE-2023-49673, CVE-2023-49674

Zasiahnuté systémy

MATLAB Plugin vo verzii staršej ako 2.11.1
Jira Plugin vo verzii straršej ako 3.12
Google Compute Engine Plugin vo verzii staršej ako 4.551.v5a_4dc98f6962
NeuVector Vulnerability Scanner Plugin vo staršej ako 2.2

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Odporúčame uistiť sa, či Vaše inštancie automatizačného servera Jenkins nevyužívajú predmetné pluginy v zraniteľnej verzii. V prípade, že áno, zabezpečte aktualizáciu všetkých komponentov, od ktorých závisí vaša aplikácia, na aktuálne verzie bez známych bezpečnostných zraniteľností.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://exchange.xforce.ibmcloud.com/vulnerabilities/272548
https://www.jenkins.io/security/advisory/2023-11-29/

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.8
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Bluetooth Core Specification - bezpečnostná zraniteľnosť

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnosti technológie Bluetooth s označením BLUFFS (Bluetooth Forward and Future Secrecy).
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje útočníkovi nachádzajúcemu sa v rovnakom sieťovom segmente prostredníctvom MITM (Man In The Middle) útoku získať neoprávnený prístup k šifrovaciemu kľúču slúžiaceho na zabezpečenie komunikácie a následne spôsobiť narušenie dôvernosti a integrity komunikácie.

Dátum prvého zverejnenia varovania

27.11.2023

CVE

CVE-2023-24023

Zasiahnuté systémy

Bluetooth Core Specification vo verzii 4.2 až 5.4 (vrátane)

Následky

Neoprávnený prístup k citlivým údajom
Neoprávnená zmena v systéme

Odporúčania

Pri produktoch, pre ktoré ešte neboli vydané bezpečnostné záplaty, odporúčame sledovať stránky výrobcu a po vydaní príslušných záplat systémy aktualizovať.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.bluetooth.com/learn-about-bluetooth/key-attributes/bluetooth-security/bluffs-vulnerability/
https://dl.acm.org/doi/pdf/10.1145/3576915.3623066
https://francozappa.github.io/post/2023/bluffs-ccs23/
https://www.rapid7.com/db/vulnerabilities/msft-cve-2023-24023/
https://nvd.nist.gov/vuln/detail/CVE-2023-24023

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 6.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Franklin Electric Fueling Systems Colibri - bezpečnostná zraniteľnosť

Popis

Spoločnosť Franklin Electric Fueling Systems vydala bezpečnostnú aktualizáciu na svoj produkt Colibri, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, autentifikovanému útočníkovi s právomocami používateľa získať neoprávnený prístup k citlivým údajom vrátane prihlasovacích údajov.

Dátum prvého zverejnenia varovania

28.11.2023

CVE

CVE-2023-5885

Zasiahnuté systémy

Colibri vo verzii firmvéru staršej ako 1.9.24.8960

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://www.cisa.gov/news-events/ics-advisories/icsa-23-331-02

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.4
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

BD FACSChorus - viacero bezpečnostných zraniteľností

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu BD FACSChorus.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje autentifikovanému útočníkovi s právomocami používateľa a fyzickým prístupom k zariadeniu získať neoprávnený prístup k citlivým údajom, vykonať neoprávnené zmeny v systéme a spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-29060, CVE-2023-29061, CVE-2023-29062, CVE-2023-29063, CVE-2023-29064, CVE-2023-29065, CVE-2023-29066

Zasiahnuté systémy

BD FACSChorus (HP Z2 G9 workstation, shipped with FACSDiscover S8 Cell Sorter) vo verzii staršej ako v5.1 (vrátane)
BD FACSChorus (HP Z2 G5 workstation, shipped with FACSMelody Cell Sorter) vo verzii staršej ako v3.1 (vrátane)

Následky

Úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť získanie prístupu k citlivým údajom je dobrou praxou zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cisa.gov/news-events/ics-medical-advisories/icsma-23-331-01

Dôležitosť	☐ **Nízka**	☒ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 5.3
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Yokogawa STARDOM - bezpečnostná zraniteľnosť

Popis

Spoločnosť Yokogawa vydala odporúčania pre mitigáciu bezpečnostnej zraniteľnosti na svoj produkt STARDOM FCN/FCJ.

Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne upravených paketov znefunkčniť administratívne rozhranie pre konfiguráciu. Zneužitie zraniteľnosti nemá žiadny vplyv na činnosť produktu.

Dátum prvého zverejnenia varovania

30.11.2023

CVE

CVE-2023-5915

Zasiahnuté systémy

STARDOM FCN/FCJ vo verzii R1.01 (vrátane) až R4.31 (vrátane)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na odkazoch v časti ZDROJE.

Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Ak je potrebný vzdialený prístup, použite virtuálnu súkromnú sieť (VPN). Administrátorom odporúčame filtrovať sieťovú komunikáciu bezpečnostnými prvkami sieťovej infraštruktúry.

Zdroje

https://web-material3.yokogawa.com/1/35463/files/YSAR-23-0003-E.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-334-02

Dôležitosť	☒ **Nízka**	☐ **Stredná**	☐ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 2.5
Klasifikácia	☒ **Neutajované / TLP(CLEAR)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mitsubishi Electric GX Works2 - dve bezpečnostné zraniteľnosti

Popis

Bezpečnostní výskumníci zverejnili informácie o zraniteľnostiach produktu GX Works2.
Zraniteľnosti spočívajú v nedostatočnom overovaní používateľských vstupov a umožňujú lokálnemu, autentifikovanému útočníkovi s právomocami používateľa prostredníctvom zaslania špeciálne upravených paketov spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

28.11.2023

CVE

CVE-2023-5274, CVE-2023-5275

Zasiahnuté systémy

GX Works2 vo všetkých verziách

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame postupovať podľa pokynov výrobcu, ktoré môžete nájsť na odkazoch v časti ZDROJE.
Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy, prílohy z neznámych zdrojov a nenavštevovali nedôveryhodné webové stránky.

Zdroje

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2023-015_en.pdf
https://www.cisa.gov/news-events/ics-advisories/icsa-23-331-03